REMARKS/ARGUMENTS

In response to the Office Action of July 12, 2005, please consider the following remarks.

In the Office Action mailed July 12, 2005, claims 1-6 and 8-28 were rejected under 35 U.S.C. § 102(e), as being anticipated by US Patent 6,233,565 (hereinafter, "Lewis et al."). Claim 7 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis and further in view of US Patent 6,598,167 (hereinafter "Devine et al.").

Claims 1-28 are currently pending in the application. Reconsideration of the instant application by the Examiner in view of the remarks below is respectfully requested.

The Prior Art

Lewis et al. discloses a secure transport for registration and password authentication. As Lewis et al. describe in the Abstract, a transaction authentication system includes authentication, wherein the client authentication module and the server authentication modules communicate via the internet connection and are authenticated to each other. Thus, Lewis et al. describe transactions between client and server. All references to encryption are performed either by the client or the server. No encryption appliance is used between the client and server to perform encryption on (only) the most sensitive parts of the transaction. Notably, Lewis et al. do not describe encryption of only a portion of a transaction.

The Prior Art Distinguished

Claim 1 includes the language "reads a configuration file to determine how to identify sensitive data within the at least one electronic transaction query" and "encrypts the sensitive data[.]" To anticipate a claim, a prior art reference must teach each and every element of a claim. Lewis et al. do not read a configuration file to

determine what parts of a transaction are sensitive. Moreover, Lewis et al. would not be motivated to determine how to identify sensitive data within a transaction because Lewis et al. do not encrypt (only) the sensitive data. Accordingly, Claim 1 is allowable over the prior art.

Claim 2 includes the language "identifying configured sensitive data elements inside the electronic request[.]" Again, Lewis et al. do not identify sensitive data within a transaction. Rather, Lewis et al. simply encrypt the entire transaction. Accordingly, Claim 2 is believed to be allowable over the prior art. Claims 3-13, which depend from Claim 2, are allowable at least for depending for an allowable base claim, and potentially for additional reasons.

Claim 3 includes the language "determining that the at least one electronic request includes sensitive data." At, for example, Col. 14, lines 35-40, Lewis et al. disclose that transactions may be encrypted. However, Lewis et al. do not make any effort to determine whether an electronic request includes sensitive data. Rather, Lewis et al. teach using SSL standard encryption, regardless of any determination. Therefore, Lewis et al. would not be motivated to determine whether a request include sensitive data, as recited in claim 3.

Claim 4 includes the language "identifying comprises identifying tags indicating that associated data is sensitive data." At, for example, Col. 37, lines 45-50, Lewis et al. describe information that is specific to a user. However, there are no identifying tags. More significantly, no tag indicates that the information is sensitive data, as recited in claim 4. As used in the specification, identifying tags refer to tags in the request that identify which data is sensitive. They do not refer to tags that can be used to identify users, such as mailing addresses, phone numbers, etc.; as are referred to in the cited portion of Lewis et al.

Claim 5 includes the language "determining that sensitive data in the electronic request includes at least one user password[.]" At, for example, col. 22, lines 58-63,

Lewis et al. describe a hash embedded inside a key file. However, Lewis et al. cannot identify a password in a transaction and append or replace it with a hash of the password. This is because Lewis et al. cannot determine that sensitive data in an electronic request includes a password, as is recited in claim 5.

Claim 6 includes the language "the at least one hash function is a keyed hash function or a non-keyed hash function." At, for example, col. 23, lines 1-10, Lewis et al. mention keys and hash functions, but the transformation of a user password with either a keyed-hash function or a non-keyed hash function is not disclosed.

Claim 7 includes the language "identifying at least one cookie of the one or more cookies that includes sensitive data[.]" Lewis et al. do not disclose how to protect cookies against inspection or modification by the user.

Claim 8 includes the language "the at least one electronic request comprises at least one protocol over Secure Socket Layer." At, for example, col. 15, lines 40-45, Lewis et al. refer to securing their particular protocol with SSL. Claim 8, which includes the limitations of claim 2, is directed to transparent encryption of selected parts of transactions on an SSL protocol. This is different than simply securing a protocol with SSL.

Claim 9 includes the language "the sensitive data comprises at least one data item selected from a group including credit card numbers, credit card information, account numbers, account information, birth dates, social security numbers, user information, and user passwords." Lewis et al. do not perform cryptographic operations on, for example, credit card numbers.

Claim 14 includes the language "determining that the at least one electronic request includes sensitive data [and] encrypting the sensitive data[.]" Again, Lewis et al. do not determine whether an electronic request includes sensitive data, and then encrypt the sensitive data. Rather, Lewis et al. encrypt an entire transaction, which obviates determining whether an electronic request includes sensitive data. Claims 15-

16, which depend from Claim 14, are allowable at least for depending for an allowable base claim, and potentially for additional reasons.

Claim 15 includes the language, "evaluating at least one request for the encrypted sensitive data[.]" At, for example, col. 14, lines 25-35, Lewis et al. describe purchase and refund requests will be encrypted for transmission. Notably, however, Lewis et al. do not describe evaluating a request for (already) encrypted sensitive data. Thus, at least at col. 14, lines 25-35, Lewis et al. are simply describing the encryption of transaction before transmission. No evaluation of a request for encrypted sensitive data is suggested or implied. Claim 15 further includes the language "decrypting the encrypted sensitive data[.]" At, for example, col. 17, lines 1-3, Lewis et al. at best describe decrypting an encrypted request. Thus, the entire request is decrypted, not just the encrypted sensitive data.

Claim 17 includes the language "determining the at least one electronic request includes a request for encrypted sensitive data and retrieving the encrypted sensitive data[.]" At, for example, col. 22, lines 40-50, Lewis et al. describe a CryptoManager, which is an object stored as a statically linked DLL. By statically linking the object to a client, it can ensure no other program has access to the DLL. However, Lewis et al. do not disclose a request for ***encrypted*** sensitive data, nor retrieving the encrypted sensitive data. Since the data stored in the CryptoManager is not encrypted, there is no need for "decrypting the encrypted sensitive data[,]" as is also recited in claim 17.

Claim 18 includes the language "at least one processing device identifies sensitive data inside the electronic request[.]" Claim 18 is allowable at least for reasons similar to those described with reference to claim 2. Claims 19-22, which depend from Claim 18, are allowable at least for depending for an allowable base claim, and potentially for additional reasons. Claims 19 and 20 are allowable at least for reasons similar to those described with reference to claim 4.

Claim 23 includes the language "at least one processing device... determines

when the at least one received electronic request includes sensitive data [and] encrypts the sensitive data[.]" Claim 23 is allowable at least for reasons similar to those described with reference to claim 14. Claim 24, which depends from Claim 23, is allowable at least for depending for an allowable base claim. In addition, claim 24 includes the language "evaluates at least one request for the encrypted sensitive data... decrypts the encrypted sensitive data[.]" Thus, claim 24 is allowable at least for reasons similar to those described with reference to claim 17.

Claim 25 is allowable for reasons similar to those described with reference to claim 17.

Claims 26 and 28 are allowable for reasons similar to those described with reference to claims 2 and/or 17.

Claim 27 is allowable for reasons similar to those described with reference to claims 1 and/or 17.

Conclusion

In view of the foregoing, the Applicants respectfully submit that the pending claims are allowable. The Applicants respectfully request the Examiner withdraw the rejections of all claims. The Applicants respectfully request that a timely Notice of Allowance be issued in this case.

Should the Examiner have any questions or comments, he is encouraged to call the undersigned at (650) 838-4305 so that any outstanding issues can be expeditiously resolved.

Respectfully submitted,
Perkins Coie LLP

Date: September 29, 2005

William F. Ahmann
Reg. No. 52,548

Correspondence Address:
Customer No. 22918
Perkins Coie LLP
P.O. Box 2168
Menlo Park, California 94026
(650) 838-4300